

	DIN EN 61508-5 (VDE 0803-5)	
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	
ICS 35.240.50	Einsprüche bis 2009-08-31 Vorgesehen als Ersatz für DIN EN 61508-5 (VDE 0803-5):2002-11 Entwurf Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln (IEC 65A/526/CDV:2008); Deutsche Fassung FprEN 61508-5:2008 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels (IEC 65A/526/CDV:2008); German version FprEN 61508-5:2008 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5 : Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité (CEI 65A/526/CDV:2008); Version allemande FprEN 61508-5:2008 Anwendungswarnvermerk Dieser Norm-Entwurf mit Erscheinungsdatum 2009-06-08 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt. Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren. Stellungnahmen werden erbeten – vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main. Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen. Gesamtumfang 93 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE	

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments FprEN 61508-5:2008 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 65A/526/CDV:2008 „Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels“ unverändert in den Entwurf FprEN 61508-5:2008 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 65A „System aspects“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium GK 914 „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme (E, E, PES) zum Schutz von Personen und Umwelt“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Änderungen

Gegenüber DIN EN 61508-5 (VDE 0803-5):2002-11 wurden folgende Änderungen vorgenommen:

- a) vertiefte Diskussion der Risiken in Anhang A;
- b) Hinzufügung eines neuen Anhanges B zur Auswahl der Methoden zur Bestimmung der Sicherheits-Integritätslevel;
- c) Aufnahme der Beschreibung der Methode der Analyse der Schutzebenen (LOPA).

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
FprEN61508-1:2008	65A/522/CDV:2008	E DIN EN 61805-1 (VDE 0803-1) in Vorbereitung	(VDE 0803-1)
FprEN61508-2:2008	65A/523/CDV:2008	E DIN EN 61805-2 (VDE 0803-2) in Vorbereitung	(VDE 0803-2)
FprEN61508-3:2008	65A/524/CDV:2008	E DIN EN 61805-3 (VDE 0803-3) in Vorbereitung	(VDE 0803-3)
FprEN61508-4:2008	65A/525/CDV:2008	E DIN EN 61805-4 (VDE 0803-4) in Vorbereitung	(VDE 0803-4)
FprEN61508-6:2008	65A/527/CDV:2008	E DIN EN 61805-6 (VDE 0803-6) in Vorbereitung	(VDE 0803-6)
FprEN61508-7:2008	65A/528/CDV:2008	E DIN EN 61805-7 (VDE 0803-7) in Vorbereitung	(VDE 0803-7)
–	ISO/IEC Guide 51:1990	–	–
–	IEC Guide 104:1997	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

E DIN EN 61805-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

E DIN EN 61805-2 (VDE 0803-2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*

E DIN EN 61805-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

— Entwurf —

E DIN EN 61508-5 (VDE 0803-5):2009-06

E DIN EN 61805-4 (VDE 0803-4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen*

E DIN EN 61805-6 (VDE 0803-6), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3*

E DIN EN 61805-7 (VDE 0803-7), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen*

Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln

Inhalt

	Seite
Einleitung	4
2 Normative Verweisungen.....	8
3 Begriffe und Abkürzungen	8
Anhang A (informativ) Risiko und Sicherheitsintegrität – Allgemeine Konzepte	9
A.1 Allgemeines	9
A.2 Notwendige Risikominderung.....	9
A.2.1 Individuelles Risiko	10
A.2.2 Gesellschaftliche Risiken.....	10
A.2.3 Kontinuierliche Verbesserung.....	10
A.2.4 Risikoprofil	11
A.3 Die Rolle der sicherheitsbezogenen E/E/PE-Systeme.....	11
A.4 Sicherheitsintegrität	11
A.5 Betriebsarten und Bestimmung des SIL	12
A.5.1 Sicherheitsintegrität und Risikominderung für Anwendungen mit niedriger Anforderungsrate.....	12
A.5.2 Sicherheitsintegrität für Anwendungen in der Betriebsart mit hoher Anforderungsrate	14
A.5.3 Sicherheitsintegrität für Anwendungen in der Betriebsart mit kontinuierlicher Anforderung	15
A.5.4 Ausfälle infolge gemeinsamer und abhängiger Ursache	16
A.5.5 Sicherheits-Integritätslevel, bei Verwendung mehrerer Schichten eines Schutzes	17
A.6 Risiko und Sicherheitsintegrität	18
A.7 Sicherheits-Integritätslevel und Software-Sicherheits-Integritätslevel	18
A.8 Zuordnung von Sicherheitsanforderungen	19
A.9 Systeme zur Schadensbegrenzung.....	21
Anhang B (informativ) Auswahl von Methoden zur Bestimmung der Sicherheits-Integritätslevel.....	22
B.1 Allgemeines	22
B.2 Quantitative Methode der SIL-Bestimmung.....	22
B.3 Die Risikograph-Methode	23
B.4 Analyse der Schutzebenen (en.: Layer of Protection Analysis (LOPA))	23
Anhang C (informativ) Konzepte für ALARP und tolerierbares Risiko.....	25
C.1 Allgemeines	25
C.2 ALARP-Modell	25
C.2.1 Einleitung	25

— Entwurf —

E DIN EN 61508-5 (VDE 0803-5):2009-06
FprEN 61508-5:2008

	Seite
C.2.2 Grenzwert für das tolerierbare Risiko	26
Anhang D (informativ) Festlegung der Sicherheits-Integritätslevel: Eine quantitative Methode	28
D.1 Allgemeines	28
D.2 Allgemeine Methode	28
D.3 Beispielrechnung	29
Anhang E (informativ) Bestimmung der Sicherheits-Integritätslevel Risikograph-Methoden	31
E.1 Allgemeines	31
E.2 Aufbau des Risikographen	31
E.3 Kalibrierung	32
E.4 Mögliche andere Risikoparameter	33
E.5 Anwendung des Risikographen: allgemeines Schema	33
E.6 Beispiel eines Risikographen	34
Anhang F (informativ) Semi-quantitative Methode, Verwendung einer Analyse der Schutzebenen (LOPA)	38
F.1 Allgemeines	38
F.1.1 Beschreibung	38
F.1.2 Anhang Verweis	38
F.1.3 Beschreibung der Methode	38
F.2 Schadensereignis	38
F.3 Schweregrad	38
F.4 Auslösende Ursache	39
F.5 Eintrittswahrscheinlichkeit	39
F.6 Schutzebenen (PLs)	42
F.6.1 Allgemeines	42
F.6.2 Grundlegendes Steuerungssystem	42
F.6.3 Alarme	42
F.7 Zusätzliche Schadensbegrenzungsmaßnahmen	43
F.8 Vorläufige Wahrscheinlichkeit für das Ereignis	43
F.9 Sicherheits-Integritätslevel (SILs)	43
Anhang G (informativ) Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise: Matrix des Ausmaßes des gefährlichen Vorfalls	45
Anhang G (informativ) Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise: Matrix des Ausmaßes des gefährlichen Vorfalls	45
G.1 Allgemeines	45
G.2 Matrix des Ausmaßes des gefährlichen Vorfalls	45
Literaturhinweise	47
Bilder	
Bild 1 – Gesamtrahmen der Betrachtung dieser Norm	7
Bild A.1 – Risikominderung: allgemeine Konzepte (Betriebsart mit niedriger Anforderungsrate)	13
Bild A.2 – Risiko- und Sicherheitsintegritätskonzepte	13

	Seite
Bild A.3 – Risikodarstellung zu Anwendungen mit hoher Anforderungsrate	15
Bild A.4 – Risikodarstellung zu Anwendungen mit kontinuierlichen Anforderungsrate	16
Bild A.5 – Darstellung von Ausfällen infolge gemeinsamer Ursache (CCFs) von Elementen im EUC-Leit- oder Steuerungssystem und Elementen im sicherheitsbezogenen E/E/PE-System	17
Bild A.6 – Gemeinsame Ursache zwischen zwei sicherheitsbezogenen E/E/PE-Systemen	18
Bild A.7 – Zuordnung der Sicherheitsanforderungen zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung	20
Bild C.1 – Tolerierbares Risiko und ALARP	26
Bild D.1 – Zuordnung der Sicherheitsintegrität: Beispiel für eine sicherheitsbezogene Schutzeinrichtung	30
Bild E.1 – Risikograph: Allgemeine Darstellung	34
Bild E.2 – Risikograph: Beispiel (zeigt nur allgemeine Prinzipien auf)	34
Bild G.1 – Matrix des Ausmaßes des gefährlichen Vorfalls: Beispiel (stellt nur die allgemeinen Prinzipien dar)	46
Tabellen	
Tabelle C.1 – Beispiel für die Risikoklassifizierung von Unfällen	27
Tabelle C.2 – Interpretation der Risikoklassen	27
Tabelle E.1 – Beispieldaten, die sich auf das Beispiel des Risikographen (Bild E.2) beziehen	35
Tabelle E.2 – Beispielkalibrierung eines allgemeinen Risikographen	36

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Elementen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme) werden in allen Anwendungsbereichen benutzt, um Nichtsicherheitsfunktionen und zunehmend auch um Sicherheitsfunktionen auszuführen. Falls Rechnersystemtechnologie wirksam und sicherheitsgerichtet eingesetzt wird, ist es wichtig, dass die für die Entscheidungsfindung Verantwortlichen ausreichende Hilfestellung bezüglich der Sicherheitsaspekte erhalten, nach denen diese Entscheidungen getroffen werden.

Diese Internationale Norm beschreibt einen allgemeinen Lösungsweg für alle Tätigkeiten während des Sicherheitslebenszyklus für Systeme, die aus elektrischen und/oder elektronischen und/oder programmierbaren elektronischen Elementen bestehen (E/E/PE) die eingesetzt werden, um Sicherheitsfunktionen auszuführen. Dieser allgemeine Lösungsweg wurde gewählt, um ein sinnvolles und konsistentes technisches Verfahren für alle elektrischen Sicherheitssysteme zu entwickeln. Ein Hauptziel ist es, die Entwicklung von anwendungsspezifischen Normen zu erleichtern.

In den meisten Situationen wird Sicherheit durch eine Anzahl von Systemen erreicht, die auf vielerlei Technologien (zum Beispiel Mechanik, Hydraulik, Pneumatik, Elektrik, Elektronik, programmierbare Elektronik) basieren. Jede Sicherheitsstrategie muss deshalb nicht nur alle Elemente innerhalb eines Einzelsystems (zum Beispiel Sensoren, Steuereinheiten und Aktoren) betrachten, sondern auch all die sicherheitsbezogenen Systeme, die einzelne Teile einer Gesamtheit sind. Da sich diese Internationale Norm mit sicherheitsbezogenen (E/E/PE) Systemen beschäftigt, kann sie einen Rahmen bereitstellen, innerhalb dessen sicherheitsbezogene Systeme, basierend auf anderen Technologien, betrachtet werden können.

Es ist berücksichtigt worden, dass eine große Vielfalt von Anwendungen, sicherheitsbezogener E/E/PE-Systeme in vielfältigen Anwendungsbereichen verwendet und diese einen weiten Bereich in Bezug auf Komplexität, Gefährdungs- und Risikopotentiale abdeckt. In jeder speziellen Anwendung hängen die erforderlichen Sicherheitsmaßnahmen von vielen anwendungsspezifischen Faktoren ab. Dadurch, dass diese Internationale Norm allgemein gehalten ist, wird die Formulierung solcher Maßnahmen in zukünftigen und in Revisionen bereits existierender, anwendungsspezifischer Internationaler Normen, ermöglicht.

Diese Internationale Norm

- betrachtet alle relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Implementierung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PE-Systeme benutzt werden, um Sicherheitsfunktionen auszuführen;
- wurde unter Berücksichtigung einer sich schnell entwickelnden Technologie entworfen. Der Betrachtungsrahmen ist ausreichend robust und ausführlich genug, um auch für zukünftige Entwicklungen verwendbar zu sein;
- ermöglicht die Erstellung anwendungsspezifischer Internationaler Normen, die sich mit sicherheitsbezogenen E/E/PE-Systemen befassen. Die Entwicklung anwendungsspezifischer Normen sollte innerhalb des Rahmens dieser Internationalen Norm zu einem hohen Grad an Übereinstimmung (zum Beispiel von zugrunde liegenden Prinzipien, Terminologie usw.) führen, sowohl innerhalb der Anwendungsbereiche als auch über die Anwendungsbereiche hinweg. Dies hat sowohl sicherheitstechnische als auch wirtschaftliche Vorteile;

ANMERKUNG 1 Hinweise [1] und [2] in den Literaturhinweisen sind anwendungsspezifische internationale Normen.

- liefert eine Methode für die Entwicklung der Spezifikation der Sicherheitsanforderungen, die notwendig ist, um die erforderliche funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen;
- verwendet einen auf dem Risiko basierenden Lösungsansatz, durch den die Anforderungen zum Sicherheits-Integritätslevel bestimmt werden können;
- führt Sicherheits-Integritätslevels für die Spezifikation der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen ein, die in dem sicherheitsbezogenen E/E/PE-System implementiert werden;

ANMERKUNG 2 Diese Norm legt weder die Anforderungen zur Sicherheitsintegrität für irgendeine Sicherheitsfunktion fest, noch bestimmt sie, wie der Sicherheits-Integritätslevel festgelegt wird. Stattdessen stellt sie einen risikobasierenden konzeptionellen Rahmen und Beispielverfahren bereit.

- legt Ausfallgrenzwerte für die von den sicherheitsbezogenen E/E/PE-Systemen auszuführenden Sicherheitsfunktionen fest, die mit den Sicherheits-Integritätsleveln verbunden sind;
- legt eine untere Grenze für die Ausfallgrenzwerte für eine Sicherheitsfunktion fest, die von einem einzelnen sicherheitsbezogenen E/E/PE-System ausgeführt wird. Für sicherheitsbezogene E/E/PE-Systeme, die
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze bei einer mittleren Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung von 10^{-5} festgelegt,
 - in der Betriebsart mit einer hohen oder ununterbrochenen Anforderungsrate betrieben werden, ist die untere Grenze der Wahrscheinlichkeit eines gefahrbringenden Ausfalls auf 10^{-9} [h⁻¹] pro Stunde festgelegt;

ANMERKUNG 3 Ein einzelnes sicherheitsbezogenes E/E/PE-System bedeutet nicht auch notwendigerweise eine ein-kanalige Architektur.

ANMERKUNG 4 Es kann für einfache Systeme möglich sein, Entwürfe von sicherheitsbezogenen Systemen mit niedrigeren Zielwerten für die Sicherheitsintegrität zu erreichen, aber diese Grenzen werden als das betrachtet, was für relativ komplexe Systeme (zum Beispiel sicherheitsbezogene programmierbare elektronische Systeme) gegenwärtig erreicht werden kann.

- legt Anforderungen für die Vermeidung und Beherrschung von systematischen Fehlern fest, die auf Erfahrung und Urteilsvermögen beruhen, das durch praktische Erfahrung in der Industrie gewonnen wurde. Wenn auch die Wahrscheinlichkeit des Auftretens systematischer Ausfälle im Allgemeinen nicht quantifiziert werden kann, erlaubt die Norm jedoch für eine festgelegte Sicherheitsfunktion den Anspruch zu erheben, dass der mit der Sicherheitsfunktion verbundene Ausfallgrenzwert als erreicht betrachtet werden kann, wenn alle Anforderungen dieser Norm erfüllt worden sind;
- lässt einen weiten Bereich von Prinzipien, Verfahren und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht das Fail-Safe-Konzept, das genutzt werden kann, wenn das Ausfallverhalten eindeutig definiert und das Niveau der Komplexität verhältnismäßig niedrig ist. Das Fail-Safe-Konzept wurde wegen des weiten Bereiches der Komplexität von sicherheitsbezogenen E/E/PE-Systemen, die im Rahmen der Norm behandelt werden, als ungeeignet betrachtet.

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508 liefert Informationen über

- die zugrunde liegenden Konzepte des Risikos und den Zusammenhang zwischen Risiko und Sicherheitsintegrität (siehe Anhang A);
- eine Anzahl von Methoden, die es ermöglichen den Sicherheits-Integritätslevel für die sicherheitsbezogenen E/E/PE-Systeme, zur Risikominderung festzulegen (siehe Anhänge B, C, D und E).

Die ausgewählte Methode hängt vom Anwendungsgebiet und den betrachteten besonderen Umständen ab. Die Anhänge B, C, D und E erläutern quantitative und qualitative Verfahren und wurden vereinfacht, um die zugrunde gelegten Prinzipien zu erläutern. Diese Anhänge wurden aufgenommen, um die allgemeinen Prinzipien einer Anzahl von Methoden aufzuzeigen, aber sie liefern keine endgültige Darstellung. Diejenigen, die die Anwendung der in den Anhängen aufgeführten Methoden beabsichtigen, sollten das angegebene Quellenmaterial zu Rate ziehen.

ANMERKUNG Für weitere Informationen bezüglich der in den Anhängen B und E dargestellten Vorgehensweisen siehe die Verweise [2] und [5] in den Literaturhinweisen. Siehe ebenfalls den Verweis [3] in den Literaturhinweisen zur Beschreibung einer zusätzlichen Vorgehensweise.

1.2 Die Teile 1, 2, 3 und 4 dieser Norm sind Sicherheits-Grundnormen, dieser Status ist aber im Zusammenhang mit einfachen sicherheitsbezogenen E/E/PE-Systemen nicht anwendbar (siehe 3.4.4 von Teil 4). Als Sicherheits-Grundnormen sind sie zur Verwendung durch technische Komitees bei der Erstellung von Normen nach *IEC Guide 104* und *ISO/IEC Guide 51* vorgesehen. Die IEC 61508 ist ebenfalls zur Verwendung als eigenständige Norm vorgesehen. Die horizontale Sicherheitsfunktion dieser internationalen Norm ist nicht anwendbar auf medizinische Einrichtungen nach der IEC 60601 Serie

1.3 Es steht in der Verantwortlichkeit eines Technischen Komitees, zur Vorbereitung und Erstellung eigener Festlegungen soweit wie möglich die Sicherheits-Grundnormen anzuwenden. In diesem Zusammenhang gilt, dass die Anforderungen, Prüfverfahren oder Prüfbedingungen dieser Sicherheits-Grundnorm nur dann anwendbar sind, wenn in den Festlegungen der Technischen Komitees darauf verwiesen wird oder diese eingebunden werden.

1.4 Bild 1 zeigt den gesamten Rahmen für die Teile 1 bis 7 der IEC 61508 und zeigt die Rolle, die IEC 61508-4 zum Erreichen der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme spielt.

— **Entwurf** —

E DIN EN 61508-5 (VDE 0803-5):2009-06
FprEN 61508-5:2008

Bild 1 – Gesamtrahmen der Betrachtung dieser Norm

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 61508-1:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electrical/programmable electronic safety-related systems*

IEC 61508-3:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations of terms*

IEC 61508-6, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

ISO/IEC Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

IEC Guide 104:1997, *Guide to the drafting of safety standards, and the role of Committees with safety pilot functions and safety group functions*

3 Begriffe und Abkürzungen

Für die Anwendung dieser Norm gelten die in IEC 61508-4 aufgeführten Begriffe und Abkürzungen.

Anhang A (informativ)

Risiko und Sicherheitsintegrität – Allgemeine Konzepte

A.1 Allgemeines

Dieser Anhang liefert Informationen über die zugrunde liegenden Konzepte des Risikos und den Zusammenhang zwischen Risiko und Sicherheitsintegrität.

A.2 Notwendige Risikominderung

Die notwendige Risikominderung (siehe 3.5.14 der IEC 61508-4) ist die Minderung des Risikos, die erreicht werden muss, um das tolerierbare Risiko für eine bestimmte Situation zu erreichen (welches entweder qualitativ¹⁾ oder quantitativ²⁾ angegeben werden darf). Das Konzept der notwendigen Risikominderung ist für die Entwicklung der Spezifikation der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme von grundlegender Bedeutung (insbesondere der Teil der Anforderungen zur Sicherheitsintegrität in der Spezifikation der Sicherheitsanforderungen). Der Zweck der Festlegung des tolerierbaren Risikos für einen bestimmten gefährlichen Vorfalls ist es darzulegen, was im Hinblick sowohl auf die Häufigkeit (oder Wahrscheinlichkeit) des gefährlichen Vorfalls als auch auf seine besonderen Auswirkungen für sinnvoll gehalten wird. Sicherheitsbezogene Systeme werden entworfen, um die Häufigkeit (oder Wahrscheinlichkeit) des gefährlichen Vorfalls und/oder die Auswirkungen des gefährlichen Vorfalls zu mindern.

Das tolerierbare Risiko hängt von vielen Faktoren ab (zum Beispiel der Schwere der Verletzung, der Anzahl der Personen, die einer Gefahr ausgesetzt sind, der Häufigkeit, mit der eine Person oder Personen einer Gefahr ausgesetzt sind und der Dauer der Einwirkung). Wichtige Faktoren werden die Empfindung und die Ansichten derjenigen sein, die dem gefährlichen Vorfall ausgesetzt sind. Zur Festlegung des tolerierbaren Risikos einer bestimmten Anwendung werden die folgenden Punkte betrachtet:

- gesetzliche Anforderungen, sowohl allgemeine als auch diejenigen, die sich direkt auf die spezifische Anwendung beziehen;
- Leitfäden der entsprechenden Behörden, die Sicherheitsregeln erstellen;
- Diskussionen und Übereinkünfte mit den verschiedenen Parteien, die an der Anwendung beteiligt sind;
- Industrienormen und -leitfäden;
- internationale Diskussionen und Übereinkünfte; die Rolle nationaler und Internationaler Normen gewinnt zunehmend an Wichtigkeit, um die Kriterien für das tolerierbare Risiko bei bestimmten Anwendungen festzulegen;
- die bestmögliche unabhängige industrielle, expertengestützte und wissenschaftliche Unterstützung durch Beratungsinstitutionen.

Bei der Bestimmung der notwendigen Anforderungen zur Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und andere Maßnahmen zur Risikominderung, sind im Hinblick auf die Erfüllung der tolerierten Häufigkeit eines gefährlichen Ereignisses, die Merkmale der Gefahr der einschlägigen Anwendung zu berücksichtigen. Die tolerierte Häufigkeit wird von den rechtlichen Anforderungen in dem Land der Anwendung und von den spezifizierten Kriterien durch Anwender-Organisationen, abhängen. Fragen, die berücksichtigt werden müssen zusammen mit, wie sie auf die sicherheitsbezogenen E/E/PE-Systeme anzuwenden sind, werden im Folgenden erörtert.

¹⁾ Um das tolerierbare Risiko zu erreichen, ist es erforderlich, die notwendige Risikominderung festzusetzen. Die Anhänge E und G der IEC 61508-5 skizzieren qualitative Methoden. Obwohl in den Beispielen zitiert ist die notwendige Risikominderung implizit durch die Angabe der SIL-Anforderung nicht ausdrücklich durch einen numerischen Wert von risikomindernden Maßnahmen erforderlich.

²⁾ Zum Beispiel, dass der gefährliche Vorfall, der zu einer bestimmten Auswirkung führt, nicht mit einer Häufigkeit von mehr als einmal in 10^8 Stunden auftreten darf.

A.2.1 Individuelles Risiko

Es werden in der Regel verschiedene Ziele für Beschäftigte und Personen im öffentlichen Bereich definiert. Die Zielvorgabe für das individuelle Risiko für die Beschäftigten bezieht sich auf die am höchsten gefährdete Person und kann ausgedrückt werden als das gesamte Risiko pro Jahr das sich bildet aus allen Tätigkeiten. Das Ziel ist auf eine hypothetische Person ausgelegt und muss daher den Anteil der Zeit berücksichtigen, den die einzelne Person bei der Arbeit verbringt. Dieses Ziel gilt für alle Risiken der gefährdeten Person und das Grenzkrisiko für eine einzelne Sicherheitsfunktion muss andere Risiken mit berücksichtigen.

Vertrauen, dass das gesamte Risiko unter ein bestimmtes Ziel reduziert wurde, kann erreicht werden durch eine Reihe von Möglichkeiten. Eine Methode besteht darin alle Risiken in Betracht zu ziehen, und die Summe aller Risiken für die am stärksten exponierte Person zu bilden. Dies kann beispielsweise in Fällen in denen eine Person vielen Risiken ausgesetzt ist schwierig werden. Hier sind rechtzeitige Entscheidungen für die Systementwicklung notwendig. Ein alternativer Ansatz ist einen bestimmten Prozentsatz des gesamten individuellen Ziel-Risikos jeder einzelnen betrachteten Sicherheitsfunktion zuzuordnen. Der zugeordnete Anteil kann in der Regel bestimmt werden aus früheren Erfahrungen mit der Art der betrachteten Anlage.

Das Ziel für eine individuelle Sicherheitsfunktion sollte auch den Konservatismus der verwendeten Methode der Risikoanalyse berücksichtigen. Alle qualitativen Methoden wie Risikographen, beinhalten einige Bewertungen kritischer Parameter die zu einem Risiko beitragen. Faktoren, die zu Risiken beitragen sind die Auswirkung des gefährlichen Vorfalles und seine Häufigkeit. Bei der Festlegung dieser Faktoren kann es nötig sein eine Reihe von Risiko-Parametern zu berücksichtigen, wie eine Anfälligkeit für einen gefährlichen Vorfall, die Anzahl der Personen die möglicherweise durch den gefährlichen Vorfall betroffen sind (d. h. Nutzungsart) und die Wahrscheinlichkeit der Vermeidung des gefährlichen Vorfalles.

Qualitative Methoden beinhalten allgemein die Entscheidung, ob ein Parameter sich innerhalb einer bestimmten Bandbreite bewegt. Die Beschreibungen der Kriterien bei der Verwendung dieser Methoden benötigen ein hohes Maß an Vertrauen, dass das Ziel für die Risiken nicht überschritten wird. Dies kann einen Einstellbereich für Grenzen aller Parameter beinhalten, so dass Anwendungen deren Parameter die Grenzbedingung einhalten, die spezifizierten Risikokriterien für die Sicherheit, erfüllen. Dieses Konzept zur Festlegung der Grenzbereiche ist sehr konservativ, denn es werden nur sehr wenige Anwendungen existieren, bei denen alle Parameter im Worst Case Bereich liegen. Das Ziel der Häufigkeit solcher Methoden kann daher höher sein als das Ziel quantitativer Methoden, es gibt ein hohes Maß an Vertrauen, dass das Gesamtrisiko aller Gefährdungen tolerierbar ist.

Wenn Personen im öffentlichen Bereich einem Risiko des Ausfalls eines sicherheitsbezogenen E/E/PE-Systems ausgesetzt sind, dann kommt in der Regel ein niedrigeres Ziel zur Anwendung.

A.2.2 Gesellschaftliche Risiken

Diese entstehen, wenn mehrere Todesfälle durch ein einzelnes Ereignis zu erwarten sind. Solche Ereignisse werden gesellschaftlich genannt, weil sie geeignet sind, eine sozialpolitische Reaktion auszulösen. Es kann bedeutende öffentliche und organisatorische Abneigung gegen die hohe Auswirkung dieser Ereignisse geben und muss in einigen Fällen berücksichtigt werden. Das Kriterium für ein gesellschaftliches Risiko wird oft ausgedrückt, als eine maximale kumulierte Häufigkeit für tödliche Verletzungen zu einer bestimmten Anzahl von Personen. Dieses Kriterium wird in der Regel in der Form einer F/N-Kurve dargestellt, wobei F die kumulative Häufigkeit einer Gefährdung und N die Anzahl der Todesfälle, die aus den Gefährdungen entstehen. Die Beziehung ist in der Regel eine gerade Linie, wenn diese auf einer logarithmischen Skala gezeichnet wird. Die Steigung der Linie wird davon abhängen, in welchem Umfang Organisationen Risiken mit höheren Auswirkungen scheuen. Die Anforderung wird sein, dass die kumulierte Häufigkeit für eine bestimmte Zahl von Todesfällen niedriger ist als die kumulierte Häufigkeit in der F/N-Kurve. (siehe Verweis [4])

A.2.3 Kontinuierliche Verbesserung

Die Grundsätze zur Verringerung des Risikos, auf einen Wert so niedrig wie vernünftiger Weise möglich, werden im Anhang C vorgestellt.

A.2.4 Risikoprofil

Bei der Entscheidung, Risikokriterien für eine bestimmte Gefährdung anzuwenden, kann es notwendig werden ein Risikoprofil über die gesamte Laufzeit der Anlage in Betracht zu ziehen. Das Restrisiko wird variieren von niedrig, nach einer Wiederholungsprüfung oder nach Durchführung einer Reparatur, bis zu einem Maximum kurz vor einer Wiederholungsprüfung. Dies sollte unter Umständen von Organisationen in Betracht gezogen werden, die die anzuwenden Risikokriterien spezifizieren. Wenn Intervalle für Wiederholungsprüfungen von Bedeutung sind, dann kann es angemessen sein, die maximale Wahrscheinlichkeit einer Gefährdung die vor einer Wiederholungsprüfung akzeptiert werden kann, zu spezifizieren. Oder die PFD (t) oder PFH (t) ist niedriger als die obere SIL-Grenze mehr als ein bestimmter Prozentsatz der Zeit (z.B. 90%).

A.3 Die Rolle der sicherheitsbezogenen E/E/PE-Systeme

Sicherheitsbezogene E/E/PE-Systeme tragen dazu bei die für das Erreichen des tolerierbaren Risikos notwendige Risikominderung zu liefern.

Ein sicherheitsbezogenes System

- beinhaltet sowohl die geforderten Sicherheitsfunktionen, die notwendig sind, einen sicheren Zustand für die EUC-Einrichtung zu erreichen oder einen sicheren Zustand für die EUC-Einrichtung aufrechtzuerhalten, und
- ist dazu vorgesehen, selbständig oder mit anderen sicherheitsbezogenen E/E/PE-Systemen, oder externen Maßnahmen zur Risikominderung die notwendige Sicherheitsintegrität für die geforderten Sicherheitsfunktionen zu erreichen (3.4.1 der IEC 61508-4).

ANMERKUNG 1 Der erste Teil der Definition gibt an, dass das sicherheitsbezogene System die Sicherheitsfunktionen ausführen muss, die in der Spezifikation der Anforderungen an die Sicherheitsfunktionen festgelegt werden. Zum Beispiel könnte die Spezifikation der Anforderungen zu den Sicherheitsfunktionen festlegen, dass bei Erreichen der Temperatur „x“ das Ventil „y“ öffnen muss, um eine Wasserzufuhr in einen Behälter zu ermöglichen.

ANMERKUNG 2 Der zweite Teil der Definition gibt an, dass das sicherheitsbezogene System die Sicherheitsfunktionen mit einem der Anwendung angemessenen Grad an Gewissheit ausführen muss, um das tolerierbare Risiko zu erreichen.

Eine Person kann ein integraler Bestandteil eines sicherheitsbezogenen E/E/PE-Systems sein. Eine Person könnte zum Beispiel von einer Anzeigetafel Informationen über den Zustand der EUC entgegennehmen und eine auf diesen Informationen beruhende sicherheitsgerichtete Handlung ausführen.

Sicherheitsbezogene E/E/PE-Systeme können in einer Betriebsart mit niedriger Anforderungsrate oder in einer Betriebsart mit hoher oder kontinuierlicher Anforderungsrate betrieben werden (siehe 3.5.12 der IEC 61508-4).

A.4 Sicherheitsintegrität

Sicherheitsintegrität ist definiert als die „Wahrscheinlichkeit eines sicherheitsbezogenen Systems, die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes zufrieden stellend auszuführen“ (3.5.2 der IEC 61508-4). Die Sicherheitsintegrität bezieht sich auf die Leistungsfähigkeit der sicherheitsbezogenen Systeme, die Sicherheitsfunktionen auszuführen (die auszuführenden Sicherheitsfunktionen sind in der Spezifikation der Anforderungen an die Sicherheitsfunktionen festgelegt).

Die Sicherheitsintegrität setzt sich aus den folgenden beiden Elementen zusammen:

- Der Sicherheitsintegrität der Hardware; derjenige Teil der Sicherheitsintegrität, der sich auf zufällige Hardwareausfälle mit gefahrbringender Ausfallart bezieht (siehe 3.5.5 der IEC 61508-4). Das Erreichen der festgelegten Stufe der Sicherheitsintegrität der Hardware kann mit einer vernünftigen Genauigkeit abgeschätzt werden. Die Anforderungen können daher unter Verwendung der üblichen Regeln für die Kombination von Wahrscheinlichkeiten zwischen den Teilsystemen aufgeteilt werden. Zum Erreichen einer angemessenen Sicherheitsintegrität der Hardware kann die Anwendung redundanter Architekturen notwendig sein.

- Die Systematische Sicherheitsintegrität: derjenige Teil der Sicherheitsintegrität, der sich auf systematische Ausfälle mit gefahrbringender Ausfallart bezieht (siehe 3.5.4 der IEC 61508-4). Obwohl die mittlere Ausfallrate für systematische Ausfälle abgeschätzt werden kann, führen die durch Entwurfsfehler und Ausfälle infolge gemeinsamer Ursache resultierenden Ausfalldaten dazu, dass die Verteilung der Ausfälle schwer vorherzusagen ist. Dies führt zu einer zunehmenden Ungewissheit in den Berechnungen der Ausfallwahrscheinlichkeiten für eine bestimmte Situation (zum Beispiel die Wahrscheinlichkeit eines Ausfalls einer sicherheitsbezogenen Schutzeinrichtung). Daher muss eine Beurteilung der Auswahl der besten Vorgehensweisen diese Ungewissheit verringern. Es ist zu beachten, dass Maßnahmen zur Reduzierung der Wahrscheinlichkeit zufälliger Hardwareausfälle keinen Einfluss auf die Wahrscheinlichkeit eines systematischen Ausfalls haben. Methoden, wie zum Beispiel die Verwendung redundanter Kanäle mit identischer Hardware, die sehr wirksam in der Beherrschung zufälliger Hardwareausfälle sind, haben nur einen geringen Nutzen bei der Reduzierung systematischer Ausfälle wie Softwarefehler.

A.5 Betriebsarten und Bestimmung des SIL

Die Betriebsart bezieht sich auf die Art und Weise, wie eine Sicherheitsfunktion verwendet werden soll, mit Bezug auf die Häufigkeit der Anforderungen an sie, diese kann entweder mit:

- **Betriebsart mit niedriger Anforderungsrate:** Wenn die Häufigkeit der Anforderungen während des Betriebs, an die Sicherheitsfunktion nicht häufiger als einmal pro Jahr erfolgt; oder
- **Betriebsart mit hoher Anforderungsrate:** Wenn die Häufigkeit der Anforderungen während des Betriebs, an die Sicherheitsfunktion häufiger als einmal pro Jahr erfolgt; oder
- **Kontinuierliche Anforderungsrate:** Wenn die Anforderung an die Sicherheitsfunktion kontinuierlich erfolgen.

Die Tabellen 2 und 3 der IEC 61508-1 zeigen die Ausfallgrenzwerte für jede der Betriebsarten im Zusammenhang mit den vier Sicherheits-Integritätsleveln. Die Betriebsarten werden in den folgenden Abschnitten weiter beschrieben:

A.5.1 Sicherheitsintegrität und Risikominderung für Anwendungen mit niedriger Anforderungsrate

Die erforderliche Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und Maßnahmen zur Risikominderung muss auf einer solchen Stufe sein, dass sichergestellt ist, dass:

- die durchschnittliche Wahrscheinlichkeit von Ausfällen bei Anforderung der sicherheitsbezogenen Systeme ausreichend niedrig ist, um zu verhindern, dass die Häufigkeit des gefahrbringenden Vorfalls die zum Erreichen des tolerierbaren Risikos geforderte Häufigkeit überschreitet; und/oder
- die sicherheitsbezogenen Systeme die Auswirkungen eines Ausfalls in dem erforderlichen Ausmaß verändern, um das tolerierbare Risiko zu erreichen.

Bild A.1 zeigt die allgemeinen Konzepte der Risikominderung. Im allgemeinen Modell ist angenommen, dass

- eine EUC und ein Steuerungssystem vorhanden ist;
- zugehörige menschliche Faktoren vorhanden sind;
- die sicherheitsbezogenen Schutzmaßnahmen folgendes umfassen
 - sicherheitsbezogene E/E/PE-Systeme;
 - andere risikomindernde Maßnahmen.

ANMERKUNG Bild A.1 ist ein verallgemeinertes Risikomodell zur Darstellung der allgemeinen Prinzipien. Um das Risikomodell für eine bestimmte Anwendung zu entwickeln, ist es notwendig, die spezifische Art und Weise, mit der die notwendige Risikominderung durch die sicherheitsbezogenen E/E/PE-Systeme und/oder andere risikomindernden Maßnahmen erreicht wird, zu berücksichtigen. Das daraus hervorgehende Risikomodell kann daher von dem in Bild A.1 gezeigten abweichen.

Die in Bild A.1 und A.2 gezeigten unterschiedlichen Risiken sind:

- **EUC-Risiko:** das Risiko, das für die festgelegten gefährlichen Vorfälle der EUC, des EUC-Leit- oder Steuerungssystems und zugehöriger menschlicher Faktoren besteht; vorgesehene sicherheitsbezogene

Schutzmerkmale werden bei der Bestimmung dieses Risikos nicht berücksichtigt (siehe 3.2.4 der IEC 61508-4);

- tolerierbares Risiko: das Risiko, das in einem gegebenen Zusammenhang basierend auf den üblichen gesellschaftlichen Wertvorstellungen tragbar ist (siehe 3.1.6 der IEC 61508-4);
- Restrisiko: im Zusammenhang mit dieser Norm ist das Restrisiko das Risiko, das für die festgelegten gefährlichen Vorfälle der EUC, des EUC-Leit- oder Steuerungssystems und zugehöriger menschlicher Faktoren verbleibt, jedoch unter Berücksichtigung der sicherheitsbezogenen E/E/PE-Systeme und anderer risikomindernden Maßnahmen (siehe auch 3.1.7 der IEC 61508-4).

Das EUC-Risiko ist eine Funktion des zur EUC selbst zugehörigen Risikos, jedoch unter Berücksichtigung der durch das EUC-Leit- oder Steuerungssystem erreichten Risikominderung. Um ungerechtfertigte Anforderungen an die Sicherheitsintegrität des EUC-Leit- oder Steuerungssystems zu verhindern, legt diese Norm Beschränkungen für die Anforderungen, die gestellt werden können, fest (siehe 7.5.2.5 der IEC 61508-1).

Die notwendige Risikominderung wird durch eine Kombination aller sicherheitsbezogenen Schutzmerkmale erreicht. Die Risikominderung, die vom Ausgangspunkt des EUC-Risikos aus notwendig ist, um das tolerierbare Risiko zu erreichen, ist in Bild A.1 gezeigt (wichtig für eine Sicherheitsfunktion die in der Betriebsart mit niedriger Anforderungsrate arbeitet).

Bild A.1 – Risikominderung: allgemeine Konzepte (Betriebsart mit niedriger Anforderungsrate)

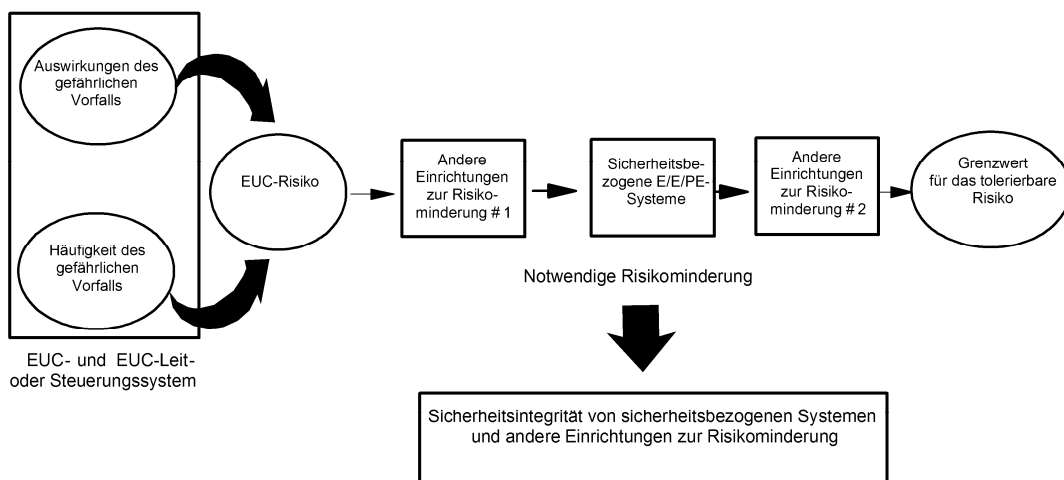


Bild A.2 – Risiko- und Sicherheitsintegritätskonzepte

A.5.2 Sicherheitsintegrität für Anwendungen in der Betriebsart mit hoher Anforderungsrate

Die erforderliche Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und andere Maßnahmen zur Risikominderung müssen auf einer Ebene sein um sicherzustellen, dass

- die durchschnittliche Wahrscheinlichkeit eines Ausfalls bei Anfrage des sicherheitsbezogenen Systems so gering ist, dass die Überschreitung der Frequenz eines gefährlichen Vorfalls zur Einhaltung des zulässigen Risikos, vermieden wird, und/oder
- die durchschnittliche Wahrscheinlichkeit des Ausfalls pro Stunde des sicherheitsbezogenen Systems so gering ist, dass die Überschreitung der Frequenz eines gefährlichen Vorfalls zur Einhaltung des zulässigen Risikos, vermieden wird.

Bild A.3 zeigt die allgemeinen Konzepte für Anwendungen in der Betriebsart mit hoher Anforderungsrate. Das Modell geht davon aus, dass

- eine EUC und ein Steuerungssystem vorhanden ist;
- zugehörige menschliche Faktoren vorhanden sind;
- die sicherheitsbezogenen Schutzmaßnahmen folgendes umfassen;
 - sicherheitsbezogene E/E/PE-Systeme in einer Betriebsart mit hoher Anforderungsrate,
 - andere risikomindernde Maßnahmen,

Verschiedene Anforderungen an die sicherheitsbezogenen E/E/PE-Systeme können wie folgt auftreten:

- Allgemeine Anforderungen durch das EUC;
- Anforderungen durch Ausfälle des EUC-Leit- oder Steuerungssystems;
- Anforderungen durch menschliches Versagen.

Wenn die Gesamtanforderungsrate aus allen Anforderungen an das System mehr als 1 pro Jahr überschreitet, dann ist dieser kritische Faktor die Rate gefahrbringender Ausfälle des sicherheitsbezogenen E/E/PE-Systems. Die Restfrequenz der Gefährdung kann die gefährliche Ausfallrate des sicherheitsbezogenen E/E/PE-Systems nie überschreiten. Sie kann niedriger sein, wenn andere Maßnahmen zur Risikominderung die Wahrscheinlichkeit von Schäden reduzieren.

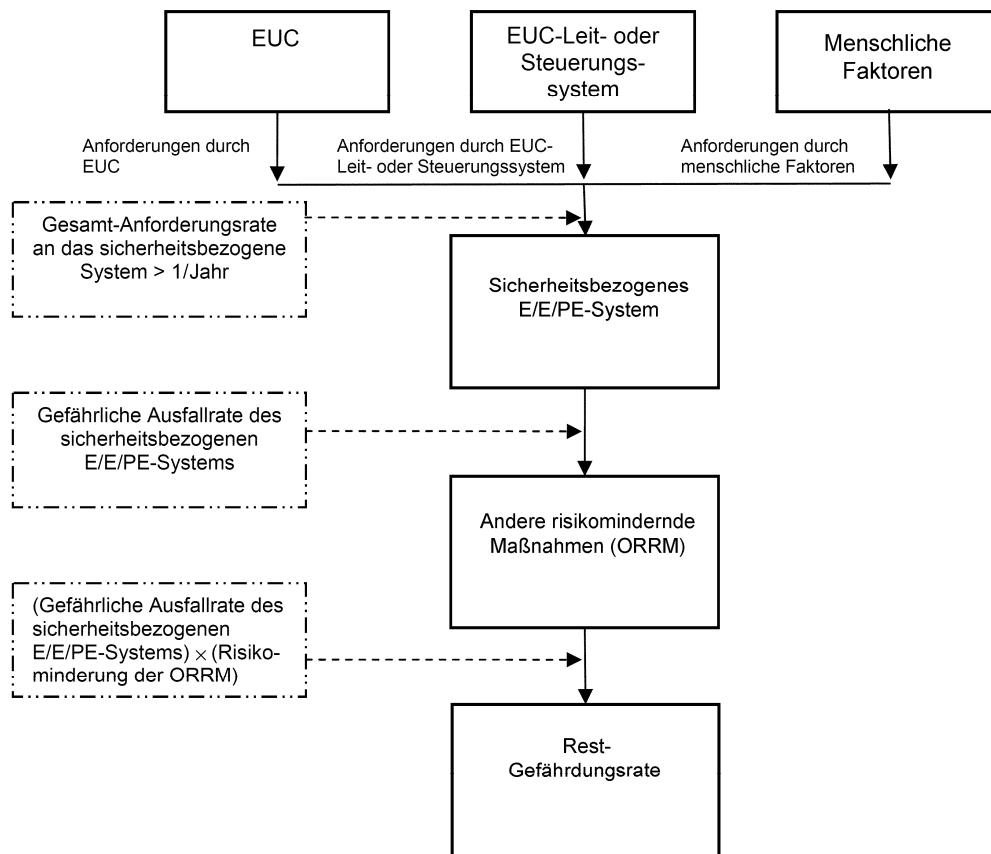


Bild A.3 – Risikodarstellung zu Anwendungen mit hoher Anforderungsrate

A.5.3 Sicherheitsintegrität für Anwendungen in der Betriebsart mit kontinuierlicher Anforderung

Die erforderliche Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und jeder anderen Maßnahme zur Risikominderung muss auf einer Ebene sein um sicherzustellen, dass die durchschnittliche Wahrscheinlichkeit des Ausfalls pro Stunde des sicherheitsbezogenen Systems so gering ist, dass die Überschreitung der Frequenz eines gefährlichen Vorfalls zur Einhaltung des zulässigen Risikos, vermieden wird.

Mit einem sicherheitsbezogenen E/E/PE-System in der Betriebsart mit kontinuierlicher Anforderung können andere risikomindernde Maßnahmen die Restfrequenz der Gefährdung, entsprechend der bereitgestellten Risikominderung, mindern. Das Modell ist in Bild A.4 gezeigt.

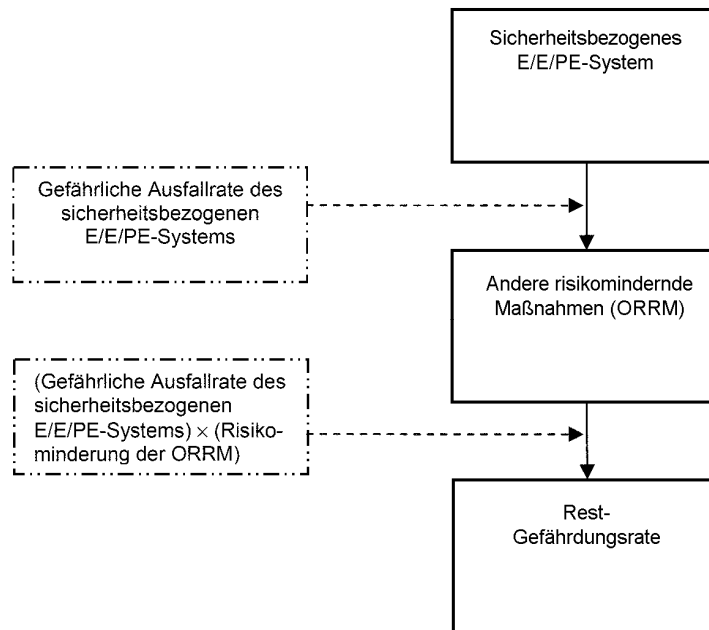


Bild A.4 – Risikodarstellung zu Anwendungen mit kontinuierlichen Anforderungsrate

A.5.4 Ausfälle infolge gemeinsamer und abhängiger Ursache

Während der Bestimmung der Sicherheits-Integritätslevel ist es wichtig Ausfälle infolge gemeinsamer und abhängiger Ursachen zu berücksichtigen. Die oben gezeigten Modelle in den Bildern A.1, A.2, A.3 und A.4 basieren auf der Grundlage, dass jedes Sicherheitssystem für die gleiche Gefährdung völlig unabhängig ist. Es gibt viele Anwendungen, bei denen dies nicht der Fall ist. Beispiele hierfür sind die folgenden:

1. wenn ein gefahrbringender Ausfall eines Elements in dem EUC-Leit- oder Steuerungssystem dazu führt, dass eine Anforderung an ein sicherheitsbezogenes System erfolgt und das sicherheitsbezogene System verwendet ein Element das aus dem gleichen Grund ausfällt. Ein Beispiel hierfür wäre, wenn ein Steuerungs- und Schutzsystem, getrennte Sensoren verwendet, aber eine gemeinsame Ursache zum Ausfall dieser beiden führen könnte (siehe Abbildung A.5);
2. wenn mehr als ein sicherheitsbezogenes System verwendet wird und innerhalb derer sind Teile der Ausrüstung gleichen Typs, so ist jedes sicherheitsbezogene System Ziel für Ausfälle infolge gleicher Ursache. Ein Beispiel wäre, wenn die gleiche Art von Sensor in zwei getrennten Schutzsystemen verwendet wird, die beide Risikominderungen für die gleiche Gefährdung bereitstellen (siehe Abbildung A.6);
3. wenn mehr als ein Schutzsystem verwendet wird, die Schutzsysteme diversitär sind, aber die Wiederholungsprüfungen erfolgen für alle Systeme gleichzeitig. In solchen Fällen wird die tatsächliche PFDavg, erreicht durch die Kombination mehrerer Systeme erheblich höher sein als die erwartete PFDavg der Multiplikation der PFDavg der einzelnen Systeme;
4. wenn das gleiche Element als Teil eines Leit- oder Steuerungssystems und eines sicherheitsbezogenen Systems verwendet wird. Wo mehr als ein Schutzsystem verwendet wird und in denen das gleiche einzelne Element als Teil von mehr als einem System verwendet wird.

In solchen Fällen ist die Wirkung der gemeinsamen Ursache/Abhängigkeit in Betracht zu ziehen. Es sollte berücksichtigt werden, ob die endgültige Anordnung in der Lage ist, die erforderliche systematische Eignung und die erforderliche Wahrscheinlichkeit gefährlicher zufälliger Hardware-Ausfallraten im Zusammenhang mit der erforderlichen gesamt Risikominderung zu erreichen. Die Wirkung von Ausfällen infolge gemeinsamer Ursache ist nur schwer zu bestimmen, und benötigt oftmals die Konstruktion von Spezialmodellen (z. B. Fehlerbaum- oder Markov-Modelle).

Die Wirkung infolge gemeinsamer Ursache ist wahrscheinlich größer in Anwendungen mit hohen Sicherheits-Integritätsleveln. In einigen Anwendungen kann Diversität erforderlich sein, so dass Auswirkungen infolge gemeinsamer Ursache minimiert werden. Es sollte jedoch darauf hingewiesen werden, dass es mit der Diversität zu Problemen beim Entwurf, der Instandhaltung und Änderung kommen kann. Die Einführung von Diversität kann zu Fehlern führen, aufgrund von Unkenntnis und mangelnder Erfahrung mit den diversen Geräten.

A.5.5 Sicherheits-Integritätslevel, bei Verwendung mehrerer Schichten eines Schutzes

Wenn mehrere Schichten eines Schutzes verwendet werden, um eine annehmbare Risiko-Frequenz zu erreichen, kann es zu Wechselwirkungen zwischen den Systemen selbst und auch zwischen den Systemen und den Ursachen einer Anforderung, kommen.

Wie bereits oben in A.5.4 erörtert, gibt es immer wieder Bedenken wegen der Gleichzeitigkeit von Prüfungen und Ausfällen infolge gemeinsamer Ursache, da diese wesentliche Faktoren sein können, wenn die Anforderungen an die Gesamt-Risikominderung hoch sind und wenn die Frequenz der Anforderungen gering ist. Die Bewertung der Wechselwirkungen zwischen den Schichten der Sicherheit und zwischen Schichten der Sicherheit und Ursachen der Anforderung kann sehr komplex sein und können die Entwicklung eines ganzheitlichen Modells nötig machen (z. B. wie in ISO / IEC 31010 ed. 1: Risk management -Risk assessment techniques, beschrieben) und auf der Grundlage, zum Beispiel eines Top-down-Ansatzes mit dem Top-Ereignis als der zulässigen Frequenz der Gefährdung. Das Modell kann alle Schichten der Sicherheit für die Berechnung der tatsächlichen Risikominderung und alle Ursachen von Anforderungen für die Berechnung der tatsächlichen Häufigkeit von Unfällen, beinhalten. Dies ermöglicht die Ermittlung von minimalen Schnittmengen (d.h. Unfall-Szenarien), zeigt die Schwachpunkte (d.h. die kleinste minimale Schnittmenge: Einzel-, Doppel-Ausfälle, usw.) in der Anordnung der Systeme und eine Systemverbesserung durch eine Analyse der Empfindlichkeiten.

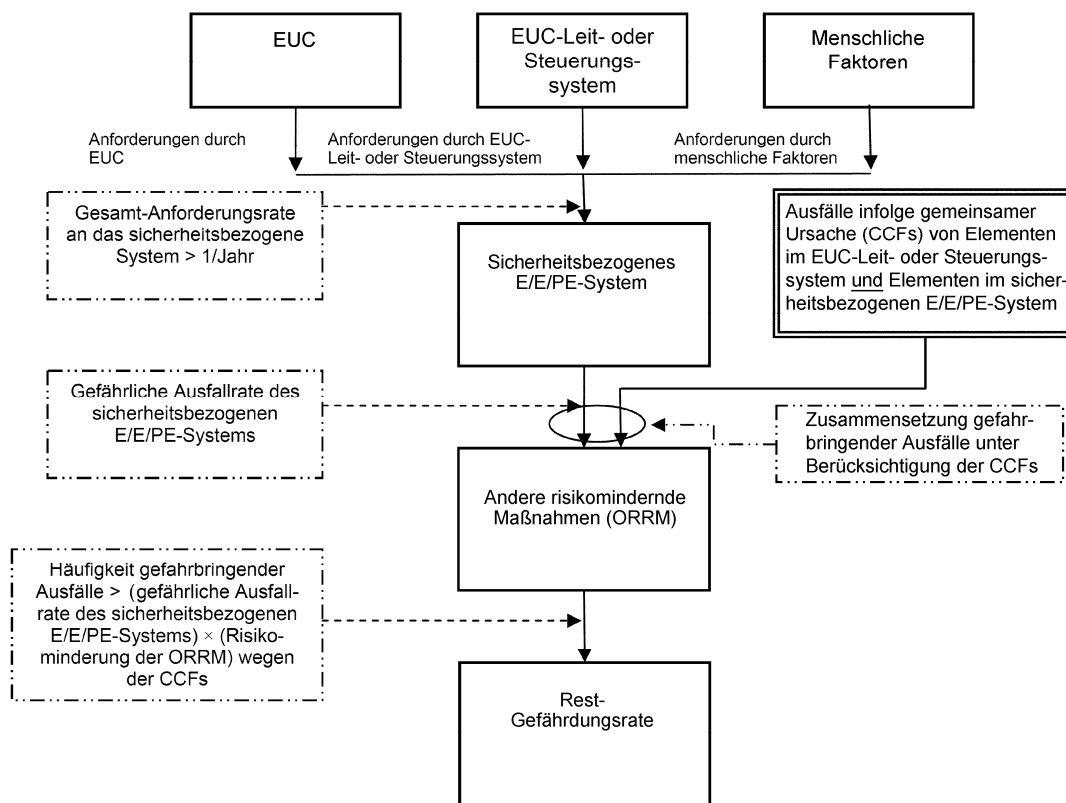


Bild A.5 – Darstellung von Ausfällen infolge gemeinsamer Ursache (CCFs) von Elementen im EUC-Leit- oder Steuerungssystem und Elementen im sicherheitsbezogenen E/E/PE-System

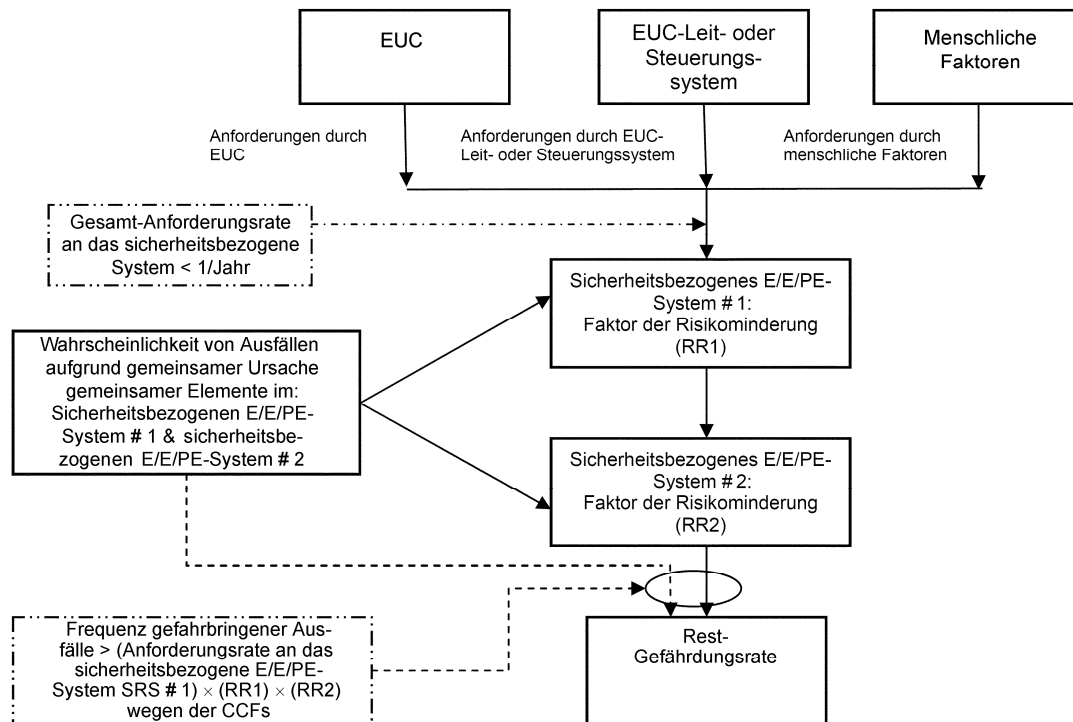


Bild A.6 – Gemeinsame Ursache zwischen zwei sicherheitsbezogenen E/E/PE-Systemen

A.6 Risiko und Sicherheitsintegrität

Es ist wichtig, dass die Unterscheidung zwischen Risiko und Sicherheitsintegrität vollständig erkannt wird. Das Risiko ist ein Maß für die Wahrscheinlichkeit und die Auswirkung eines bestimmten auftretenden gefährlichen Vorfalls. Es kann für unterschiedliche Situationen ausgewertet werden (EUC-Risiko, notwendige Risikominderung, um das tolerierbare Risiko zu erreichen, tatsächliches Risiko (siehe Bild A.1)). Das tolerierbare Risiko wird bestimmt unter Berücksichtigung des in A.2 beschriebenen Sachverhalts. Die Sicherheitsintegrität bezieht sich nur auf die sicherheitsbezogenen E/E/PE-Systeme und andere risikomindernde Maßnahmen und ist ein Maß für die Wahrscheinlichkeit dieser Systeme/Einrichtungen, die notwendige Risikominderung in Bezug auf die festgelegten Sicherheitsfunktionen zufrieden stellend zu erreichen. Sobald das tolerierbare Risiko festgelegt und die notwendige Risikominderung bestimmt worden ist, können die Anforderungen zur Sicherheitsintegrität für die sicherheitsbezogenen Systeme zugeordnet werden (siehe 7.4, 7.5 und 7.6 der IEC 61508-1).

ANMERKUNG Die Zuordnung ist notwendigerweise iterativ, um den Entwurf so zu optimieren, dass die verschiedenen Anforderungen erfüllt werden.

A.7 Sicherheits-Integritätslevel und Software-Sicherheits-Integritätslevel

Um den weiten Bereich der notwendigen Risikominderungen, den sicherheitsbezogene Systeme erreichen müssen, abzudecken, ist es nützlich, über eine Anzahl von Sicherheits-Integritätsleveln zur Erfüllung der Anforderungen der Sicherheitsintegrität der Sicherheitsfunktionen, die den sicherheitsbezogenen Systemen zugewiesen sind, zu verfügen. Software-Sicherheits-Integritätslevel werden als Grundlage für die Spezifikation der Anforderungen zur Sicherheitsintegrität von Sicherheitsfunktionen, die teilweise durch die sicherheitsbezogene Software realisiert werden, verwendet. Die Spezifikation der Anforderungen zur Sicherheitsintegrität sollte den Sicherheits-Integritätslevel für die sicherheitsbezogenen E/E/PE-Systeme bestimmen.

In dieser Norm sind vier Sicherheits-Integritätslevel festgelegt, wobei der Sicherheits-Integritätslevel 4 die höchste und der Sicherheits-Integritätslevel 1 die niedrigste Stufe ist.

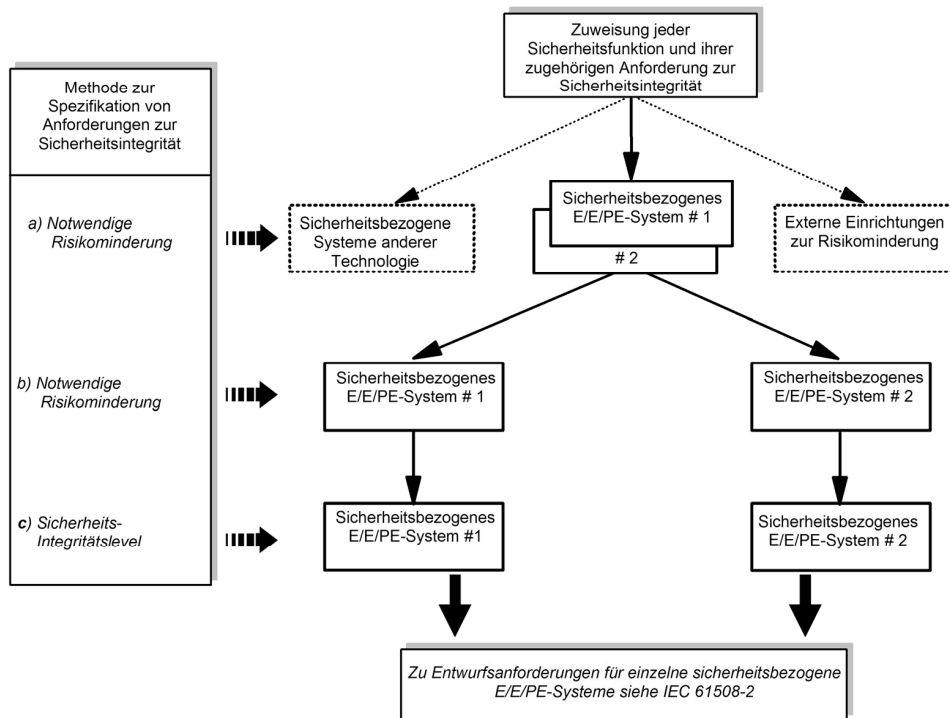
Die Versagens- und Ausfallgrenzwerte für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 der IEC 61508-1 angegeben. Zwei Parameter sind angegeben, einer für sicherheitsbezogene Systeme, die in einer Betriebsart mit niedriger Anforderungsrate betrieben werden, und einer für sicherheitsbezogene Systeme, die in einer Betriebsart mit hoher oder kontinuierlicher Anforderungsrate betrieben werden.

ANMERKUNG Für sicherheitsbezogene Systeme, die in einer Betriebsart mit niedriger Anforderungsrate betrieben werden, ist das interessierende Maß für die Sicherheitsintegrität die Wahrscheinlichkeit, die entworfene Funktion auf Anforderung nicht auszuführen. Für sicherheitsbezogene Systeme, die mit einer Betriebsart mit hoher oder kontinuierlicher Anforderungsrate betrieben werden, ist das interessierende Maß für die Sicherheitsintegrität die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (siehe 3.5.12 und 3.5.13 der IEC 61508-4).

A.8 Zuordnung von Sicherheitsanforderungen

Die Zuordnung von Sicherheitsanforderungen (sowohl der Sicherheitsfunktionen als auch der Anforderungen zur Sicherheitsintegrität) zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung wird in Bild A.7 dargestellt (dies ist identisch zu Bild 6 der IEC 61508-1). Die Anforderungen an die Phase der Zuordnung der Sicherheitsanforderungen sind in 7.6 der IEC 61508-1 enthalten.

Die Methoden für die Zuordnung der Anforderungen zur Sicherheitsintegrität zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung hängen zuallererst davon ab, ob die notwendige Risikominderung in einer numerischen oder qualitativen Art und Weise festgelegt ist. Diese Methoden werden als quantitative bzw. qualitative Methoden bezeichnet (siehe Anhänge B, C, D und E).



ANMERKUNG 1 Anforderungen an die Sicherheitsintegrität sind jeder Sicherheitsfunktion vor der Zuweisung zugeordnet (siehe 7.5.2.6 von IEC 61508-1).

ANMERKUNG 2 Eine Sicherheitsfunktion kann mehr als einem sicherheitsbezogenen System zugeordnet werden.

Bild A.7 – Zuordnung der Sicherheitsanforderungen zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung

A.9 Systeme zur Schadensbegrenzung

Systeme zur Schadensbegrenzung werden aktiv, im Falle des vollständigen oder teilweisen Ausfalls anderer sicherheitsbezogener Systeme wie z. B. E/E/PE-Sicherheits-Systeme. Das Ziel ist eher die Verringerung der Auswirkungen im Zusammenhang mit einem gefährlichen Vorfall als dessen Häufigkeit. Zu Beispielen für Systeme zur Schadensbegrenzung gehören Feuer- und Gas-Systeme (Erkennung von Feuer / Gas- und nachgeordnete Maßnahmen, um das Feuer zu löschen (z. B. durch Wasserflutung) und Airbag-Systeme in einem Auto).

Bei der Bestimmung der Anforderungen der Sicherheitsintegrität sollte berücksichtigt werden, dass, wenn die Entscheidungen über die Schwere der Auswirkungen getroffen werden, nur die erhöhten Auswirkungen zu berücksichtigen sind. Das bedeutet, Bestimmung der Zunahme der Schwere der Auswirkungen, wenn die Funktion nicht in Betrieb ist, gegenüber wenn diese wie vorgesehen arbeitet. Dies kann erfolgen, indem zunächst die Konsequenzen betrachtet werden, wenn das System nicht wie vorgesehen funktioniert und dann betrachtet, welchen Unterschied es ausmacht wenn die Systeme zur Schadensbegrenzung ordnungsgemäß arbeiten. Bei der Berücksichtigung der Auswirkungen, wenn das System nicht wie vorgesehen funktioniert, wird sich in der Regel eine Reihe von Ergebnissen mit unterschiedlichen Wahrscheinlichkeiten ergeben.

ANMERKUNG Die Anleitung zur Bestimmung des Sicherheits-Integritätslevels für Feuer-, Gas- und Notabschaltungs-Systeme ist im Anhang B der ISO-10418, Petroleum and natural gas industries. – Analysis, design and testing of basicsurface process safety systems on offshore production installations – Requirements and Guidelines, enthalten.

Anhang B (informativ)

Auswahl von Methoden zur Bestimmung der Sicherheits-Integritätslevel

B.1 Allgemeines

Dieser Anhang enthält eine Reihe von Verfahren die zur Bestimmung des Sicherheits-Integritätslevels verwendet werden können. Keines der Verfahren eignet sich für alle Anwendungen und die Benutzer wählen das am besten geeignete aus. Bei der Auswahl der am besten geeigneten Verfahren sollten die folgenden Faktoren berücksichtigt werden.

1. Die Risiko-Akzeptanzkriterien die zu erfüllen sind. Einige der Verfahren werden nicht geeignet sein, wenn erforderlich nachzuweisen, dass das Risiko so weit wie vernünftigerweise möglich reduziert wurde.
2. Die Betriebsart der Sicherheitsfunktion. Einige Verfahren sind nur für die Betriebsart mit niedriger Anforderungsrate, geeignet.
3. Das Wissen und die Erfahrung der Personen, die die SIL-Bestimmung durchführen und wie der traditionelle Ansatz in dem Bereich gewesen war.
4. Das notwendige Vertrauen, das das sich ergebende Restrisiko die spezifizierten Kriterien der Anwender-Organisation erfüllt. Einige der Methoden können verbunden werden zu quantifizierten Zielen, einige Ansätze sind aber nur qualitativ.
5. Es kann mehr als eine Methode verwendet werden. Eine Methode kann für eine Vorauswahl verwendet werden, gefolgt von einem anderen strengeren Ansatz, wenn die Vorauswahl die Notwendigkeit eines hohen Sicherheits-Integritätslevels zeigt.
6. Die Schwere der Auswirkungen. Strengere Methoden können ausgewählt werden wenn die Auswirkungen mehrere Todesopfer beinhalten.
7. Ob gemeinsame Ursachen zwischen den sicherheitsbezogenen E/E/PE-Systemen oder zwischen dem sicherheitsbezogenen E/E/PE-System und den Ursachen der Anforderungen, bestehen.

Unabhängig von der angewandten Methode sollten alle gemachten Annahmen für das zukünftige Management der Sicherheit aufgezeichnet werden. Alle Entscheidungen sollten aufgezeichnet werden, damit die SIL-Beurteilung verifiziert und einer unabhängigen Beurteilung der funktionalen Sicherheit unterzogen werden kann.

B.2 Quantitative Methode der SIL-Bestimmung

Die quantitative Methode ist in Anhang D beschrieben. Sie kann zusammen mit der ALARP-Methode in Anhang C verwendet werden.

Die quantitative Methode kann sowohl für einfache als auch komplexe Anwendungen verwendet werden. Bei komplexen Anwendungen können Fehlerbäume konstruiert werden um das Gefährdungsmodell darzustellen. Das maximale Ereignis wird in der Regel ein oder mehrere Todesopfer sein und eine Logik entworfen, um die Ursachen der Anforderungen und Ausfälle der sicherheitsbezogenen E/E/PE-Systeme darzustellen, die zu dem maximalen Ereignis führen. Es stehen Software-Werkzeuge zur Verfügung gemeinsame Ursachen zu modellieren, wenn die gleiche Art von Ausrüstung, für die Steuerungs- und Schutz-Funktionen, verwendet wird. In einigen komplexen Anwendungen kann ein einzelnes Ausfallereignis an mehr als einer Stelle im Fehlerbaum auftreten. Dies erfordert die Durchführung einer bool'schen Reduzierung. Die Werkzeuge unterstützen auch die Anfälligkeitsanalyse um die beherrschenden Faktoren des Einflusses auf die Häufigkeit des maximalen Ereignisses zu zeigen. Der SIL kann begründet werden durch die Bestimmung der erforderlichen Risikominderung um das tolerierbare Risiko-Kriterium zu erreichen.

Die Methode ist geeignet für Sicherheitsfunktionen, in der Betriebsart mit kontinuierlicher/höher- und der Betriebsart mit niedriger Anforderungsrate. Diese Methode ergibt in der Regel geringe SILs, da das Risikomodell speziell für jede Anwendung und numerische Werte entworfen worden ist, um jeweils einen Risikofaktor darzustellen, statt der numerischen Bereiche die in kalibrierten Risikographen verwendet werden. Quantitative Methoden erfordern jedoch die Konstruktion eines speziellen Modells für jeden gefährlichen Vorfall.

Die Modellierung erfordert Geschick, Werkzeuge und Kenntnisse über die Anwendung und kann erhebliche Zeit zur Entwicklung und zur Überprüfung erfordern.

Die Methode erleichtert den Nachweis, dass das Risiko so weit wie vernünftigerweise möglich reduziert wurde. Dies kann geschehen, durch Berücksichtigung von Möglichkeiten für eine weitere Risikominderung, der Integration von zusätzlichen Einrichtungen in das Fehlerbaum-Modell und dann die Bestimmung der Verringerung des Risikos und der Vergleich mit den Kosten für diese Möglichkeit.

B.3 Die Risikograph-Methode

Die qualitative Methode des Risikographen ist in Anhang E beschrieben. Die Methode ermöglicht es, den Sicherheits-Integritätslevel auf der Kenntnis der Risikofaktoren die mit dem EUC-Leit- oder Steuerungssystem verbunden sind, zu bestimmen. Es wird eine Reihe von Parametern eingeführt, die zusammen die Art der Gefährdungssituation beschreiben, wenn sicherheitsrelevante Systeme versagen oder nicht zur Verfügung stehen. Ein Parameter wird aus einem Satz von vieren gewählt, und die ausgewählten Parameter werden dann so kombiniert, um den der Sicherheitsfunktion zugeordneten Sicherheits-Integritätslevel, zu bestimmen. Die Methode wurde ausführlich im Maschinensektor, siehe ISO 14121-2 und Anhang A der ISO 13849-1, verwendet.

Die Methode kann qualitativ sein, in diesem Fall ist die Auswahl der Parameter subjektiv und erfordert ein erhebliches Urteilsvermögen. Das Restrisiko kann nicht durch die Kenntnis der Werte der Parameter berechnet werden. Es ist nicht geeignet, wenn eine Organisation fordert, dass Restrisiko auf einen bestimmten, quantitativen, Wert zu reduzieren.

Die Beschreibung der Parameter kann numerische Werte beinhalten, die sich durch die Kalibrierung des Risikographen, gegen numerische tolerierte Risikokriterien, herleiten. Das Restrisiko lässt sich, aus den verwendeten numerischen Werten der Parameter, berechnen. Es ist geeignet, wenn eine Organisation Vertrauen fordert, dass das Restrisiko auf einen bestimmten quantitativen Wert reduziert ist. Die Erfahrung hat gezeigt, dass die Verwendung der Methode eines kalibrierten Risikographen zu hohen Sicherheits-Integritätslevel führen kann. Dies liegt daran, dass die Kalibrierung in der Regel mit verwendeten Worst Case Werten der einzelnen Parameter durchgeführt wird. Jeder Parameter hat den Bereich einer Dekade, so dass für Anwendungen, bei denen alle Parameter für den Bereich Durchschnittswerte sind, wird der SIL eine Dekade höher sein als das notwendige tolerierbare Risiko. Das Verfahren wird umfangreich in der Prozess- und dem Offshore-Sektor eingesetzt.

Die Risikograph-Methode berücksichtigt nicht, Ausfälle infolge gemeinsamer Ursache zwischen den Ursachen von Anforderungen und der Ursache des Ausfalls des sicherheitsbezogenen E/E/PE-Systems oder gemeinsame Ursachen mit anderen Schichten eines Schutzes.

B.4 Analyse der Schutzebenen (en.: Layer of Protection Analysis (LOPA))

Die grundlegende Methode ist in einer Reihe von Büchern beschrieben und das Verfahren kann in einer Reihe von verschiedenen Formen erfolgen. Eine Technik, die für die SIL-Bestimmung verwendet werden kann, ist im Anhang F beschrieben.

Das Verfahren ist quantitativ und der Anwender hat die zulässigen Häufigkeiten für jede Auswirkung und Schweregrad festzulegen. Es erfolgt eine numerische Gutschrift für die Schutzebenen, die die Häufigkeit der individuellen Ursachen für Anforderungen reduzieren. Nicht alle Schutzebenen sind für alle Ursachen von Anforderungen zuständig, so dass das Verfahren für komplexere Anwendungen verwendet werden kann. Die den Schutzebenen zugeordneten numerischen Werte können auf die nächste signifikante Zahl oder den nächsten signifikanten Dekadebereich aufgerundet werden. Wenn numerische Werte von Schutzebenen auf die nächste signifikante Zahl gerundet sind, dann ergibt die Methode im Durchschnitt geringere Anforderungen an die Risikominderung und niedrigere SIL-Werte als kalibrierte Risikographen.

Da numerische Ziele, bestimmten Auswirkungen, Schweregraden zugeordnet sind, kann der Anwender darauf vertrauen, dass das Restrisiko die Firmenkriterien erfüllt.

Wie beschrieben, ist die Methode nicht geeignet für Funktionen, die in der Betriebsart mit kontinuierlicher Anforderung betrieben werden und berücksichtigt nicht den Ausfall infolge gemeinsamer Ursache zwischen

— **Entwurf** —

E DIN EN 61508-5 (VDE 0803-5):2009-06
FprEN 61508-5:2008

Ursachen der Anforderungen und dem sicherheitsbezogenen E/E/PE-System. Die Methode kann jedoch angepasst werden und eignet sich dann für solche Fälle.